INTEGER SUB-DECOMPOSITION (ISD) METHOD FOR ELLIPTIC CURVE SCALAR MULTIPLICATION

RUMA KAREEM K. AJEENA

UNIVERSITI SAINS MALAYSIA
2015

INTEGER SUB-DECOMPOSITION (ISD) METHOD FOR ELLIPTIC CURVE SCALAR MULTIPLICATION

by

RUMA KAREEM K. AJEENA

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy

March 2015

DEDICATIONS

To the soul of my late father,

to my mother,

to my husband,

and to all my family,

who I love very much, I dedicate this work.

Ruma Kareem K. Ajeena

11-11-2014

ACKNOWLEDGEMENTS

Above all, my thanks and gratitude to Allah, the almighty who awarding me the health, opportunity, and courage to be able to accomplish this work.

I would like to present thanks to my Supervisor Associate Professor Dr. Hailiza Kamarulhaili for her cooperation. Also, my thanks goes to Dr. Ang Miin Huey for her cooperation to allow me to attend her lectures in coding theory and further linear algebra.

I'm very grateful and I would like to give my thanks to all my family, especially, my mother, my husband and all other for constantly support and sacrifice during the lengthy performance of this thesis.

To all who contribute to the development of this work will offer thanks and gratitude. I'm very grateful and I would like to give my thanks to Prof. Dr. Andreas Enge and Prof. Dr. Abderrahmane Nitaj for their opinion about this work. And also Prof. Dr. Darrel Hankerson for his help to answer some my inquiries. In addition to, my thanks goes to Dr. Rand Al-Faris for her cooperation at the beginning of my study.

I would like to thanks Prof. Dr. Ahmad Izani Md. Ismail, Dean of the School of Mathematical Sciences- University Sains Malaysia, all other staff and technicians, especially Mr. Syed M. Hussein for their cooperation. Also, my thanks goes to my professors, colleagues and all staff at the School of Mathematics-Babylon University, Iraq, to give me the opportunity to complete my Ph.D study and their cooperation with me.

Further, to all my friends in every where, especially Dr. Mustafa Atheer, and who help, wish and pray to me all the best, I present my thanks and respect.

Ruma Kareem K. Ajeena

11-11-2014

TABLE OF CONTENTS

MATHEMATICAL SYMBOLS

$\mathbb{N}$	The set of natural numbers
$\mathbb{Z}$	The set of integers
$\mathbb{Q}$	The set of rational numbers
K	Any field
$Char(K)$	The characteristic of a field K
$GF(p)$ or F_p	Prime finite field
p	A prime number characteristic of a prime field
L	Lattice
$L(B)$	Lattice generated by a matrix B
L_s	Sub-lattice
a^{-1}	Multiplicative inverse of in F_p
E	Elliptic curve
$deg(E)$	The degree of polynomial E
$E(K)$	The set of points on an elliptic curve
$E[n]$	The set of torsion points
	curve defined over a field K
D_E	Discriminant of E
$j(E)$	j-invariant of elliptic curve E
$E(F_p)$	Elliptic curve group over prime field
$\#E(F_p)$	The order of elliptic curve group over prime field

P, Q	Points on elliptic curve E defined over a field K
n	Prime order of elliptic point P
O_E	Point at infinity
$\langle P \rangle$	cyclic subgroup of $E(F_p)$
$\simeq$	Isomorphism
T	The group homomorphism from $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/n$
$ker(T)$	The kernel of homomorphism T
I	A field inversion
M	A field multiplication
S	A field squaring
$+_E$	Addition operation on elliptic curve
A	Elliptic curve point addition
D	Elliptic curve point doubling
$\mathbb{Z} \times \mathbb{Z}$	Lattice in two dimensions
$\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/n$ or $\mathbb{Z}n$	The set of integer modulo n
$\{v_1, v_2\}$	GLV generator
$\{v_3, v_4\} \& \{v_5, v_6\}$	ISD generators
$\|\|v\|\|$	Euclidean norm of the vector v
$gcd(a,b)$	Greatest common divisor between integers a and b
$\mathfrak{D} = \langle d_j \rangle = \langle gcd(x_j, y_j) \rangle$	Positive sequence of gcds, where $j = 1, 2, ..., m$

$\mathfrak{a} = \langle a_j \rangle, \mathfrak{b} = \langle b_j \rangle, \mathfrak{C} = \langle c_j \rangle$	Tuples of j-integers
$\psi(P)$	Efficiently computable endomorphism
kP	Elliptic curve scalar multiplication
k	The scalar in a scalar multiplication kP
w, w_j	The window width values of wNAF
$aP + bQ$	Multiple scalar multiplication
$\Sigma a_j P j$	Interleaving computation method
$O(\sqrt{n})$	big O notation
C	The value in the upper bound $C\sqrt{n}$
$k_{GLV}(n-1)$	The number of GLV scalars k in the interval [1,n-1]
$k_{ISD}(n-1)$	The number of ISD scalars k in the interval [1,n-1]
$R_{GLV}(k)$	The ratio of the GLV scalars in the interval [1,n-1]
$R_{ISD}(k)$	The ratio of the ISD scalars in the interval [1,n-1]
$Percentage_{GLV}(kP)$	The successful percentage of computation of the GLV method
$Percentage_{ISD}(kP)$	The successful percentage of computation of the ISD method
C_{EEA}	The cost of extended Euclidean algorithm
$C_{GLV\,generator}$	The cost of GLV generator
$C_{Decomposing\ k}$	The cost of decomposing k
$C_{\psi(P)}$	The cost of efficiently computable endomorphism
$C_{w_j NAF(a_j)}$	The cost of w_jNAF expansion
$C_{\sum_{j=1}^{m} a_j P_j}$	The cost of m-interleaving computation method
$C_{GLV Method}$	The cost of GLV method

C_{PGEEA}	The cost of the parallel generalized extended Euclidean algorithm
C_{PNCP}	The cost of the parallel necessary condition part
$C_{ISD}generators$	The cost of ISD generators
$C_{Sub-decomposing\ k}$	The cost of sub-decomposing k
$C_{\psi_1(P)\&\psi_2(P)}$	The cost of the parallel computation of two endomorphisms
$C_{TwoInterleaving}$	The cost of 2-interleaving computation method
$C_{OneInterleaving}$	The cost of 1-interleaving computation method
$C_{ISDMethod}$	The cost of ISD method
$k_{GLV-ISD}(n-1)$	The number of GLV-ISD scalars k in the interval [1,n-1]
$R_{GLV-ISD}(k)$	The ratio of the GLV-ISD scalars in the interval [1,n-1]
$Percentage_{GLV-ISD}(kP)$	The successful percentage of computation of the GLV-ISD method
$C_{sc}(GLV-ISD)$	The cost of GLV-ISD method in serial computation
$C_{pc}(GLV-ISD)$	The cost of GLV-ISD method in parallel computation
Z	The dimension of tuples of variables r_i, t_i and s_i
Z_1	The dimension of tuples of variables r_{i_1}, t_{i_1} and s_{i_1}
Z_2	The dimension of tuples of variables r_{i_2}, t_{i_2} and s_{i_2}

ABBREVIATIONS

ECCs	The elliptic curve cryptosystems
ECADD	The elliptic curve addition
ECDBL	The elliptic curve doubling
DLP	The Discrete Logarithm Problem (DLP)
SVP	The Shortest Vector Problem
CVP	The Closest Vector Problem
GLV	The Gallant-Lambert-Vanstone
ISD	The integer sub-decomposition
GLV-ISD	The Hybrid method of the Gallant-Lambert-Vanstone and Integer Sub-Decomposition
EEA	Extended Euclidean algorithm
GEEA	The generalization of extended Euclidean algorithm
PGEEA	The parallel generalization of extended Euclidean algorithm
GDA	The generalization of Division algorithm
*w*NAF	The window non-adjacent form
GEA	The generalization of Euclidean algorithm

LIST OF TABLES

LIST OF FIGURES

Page

KAEDAH SUB-PELERAIAN INTEGER BAGI PERKALIAN SKALAR LENGKUNG ELIPTIK

ABSTRAK

Dalam kajian ini, kaedah baru yang dipanggil sub-peleraian integer (ISD) berdasarkan prinsip Gallant, Lambert dan Vanstone (GLV) bagi mengira perkalian skalar kP berbentuk lengkung elips E melebihi kawasan terbatas utama F_p yang mempunyai pengiraan endomorphisms ψ_j yang efisyen bagi $j = 1,2$, menghasilkan nilai yang dihitung sebelum ini untuk $\lambda_j P$, di mana $\lambda_j \in [1, n-1]$ telah dicadangkan. Jurang utama dalam kaedah GLV telah ditangani dengan menggunakan kaedah ISD. Skalar k dalam kaedah ISD telah dibahagikan dengan menggunakan rumusan

$$k \equiv k_{11} + k_{12}\lambda_1 + k_{21} + k_{22}\lambda_2 \ (mod\ n),$$

dengan $max\{|k_{11}|, |k_{12}|\} \leq \sqrt{n}$ dan $max\{|k_{21}|, |k_{22}|\} \leq \sqrt{n}$. Oleh yang demikian formula perkalian kP scalar ISD boleh dinyatakan seperti berikut:

$$kP = k_{11}P + k_{12}\psi_1(P) + k_{21}P + k_{22}\psi_2(P).$$

Nilai-nilai bagi sub-skalar k_{11}, k_{12}, k_{21} dan k_{22} telah dikira dengan menyelesaikan masalah vektor pendek (SVP) dalam sub-kekisi, iaitu, kernel dari T homomorfisma, $kerT$ bagi dua dimensi kekisi $\mathbb{Z} \times \mathbb{Z}$. Selain itu, batas atas bagi vektor "kernel" untuk

pengurangan "map" ISD telah dibuktikan dengan menggunakan karakter polinomial $p_j(X)$ untuk endomorphisms ψ_j bagi $j = 1,2$ yang mempunyai satu atau dua darjah. Berdasarkan pada taburan skalar ISD k dalam selang $[1, n-1]$, perbandingan peningkatan peratusan bagi pengiraan kP kaedah ISD yang terhasil dengan kaedah GLV telah ditentukan. Dalam kajian ini, algoritma ISD melalui pengiraan serentak umum bagi w_jNAF untuk $j = 1,2,3,4$ dan algoritma- algoritma interleaving lanjutan dengan menggunakan dua model telah dilaksanakan. Berdasarkan pelaksanaan algoritma ISD, kerumitan pengiraan ISD telah ditentukan berdasarkan kos lengkung elips dan operasi medan terhingga melalui satu operasi kitaran berbanding dengan kaedah GLV .

Pencapaian terpenting dalam penyelidikan ini adalah berasaskan teori matematik yang konkrit dan teguh relevan dengan teknik ISD. Takrif-takrif, teorem-teorem, lema-lema dan korolari-korolari baharu dibangunkan, dibincangkan serta dibuktikan dalam penyelidikan ini. kaedah baru GLV-ISD yang diubahsuai menggabungkan kaedah GLV dan ISD, juga telah dicadangkan untuk mengira perkalian skalar kP. Dengan menggunakan kaedah gabungan ini, sebahagian besar peratusan pengiraan kP yang terhasil boleh ditentukan dalam perbandingan antara kaedah GLV atau ISD secara berasingan. Semue algritma dalam kaedah ISD dan GLV-ISD hibrid dilaksanakan ,enggunakan perisian Sage.

INTEGER SUB-DECOMPOSITION (ISD) METHOD FOR ELLIPTIC CURVE SCALAR MULTIPLICATION

ABSTRACT

In this study, a new method called integer sub-decomposition (ISD) based on the Gallant, Lambert, and Vanstone (GLV) method to compute the scalar multiplication kP of the elliptic curve E over prime finite field F_p that have efficient computable endomorphisms ψ_j for $j = 1,2$, resulting in pre-computed values of $\lambda_j P$, where $\lambda_j \in [1, n-1]$ has been proposed. The major gaps in the GLV method are addressed using the ISD method. The scalar k, on the ISD method is decomposed using the formulation

$$k \equiv k_{11} + k_{12}\lambda_1 + k_{21} + k_{22}\lambda_2 \ (mod\ n),$$

with $max\{|k_{11}|, |k_{12}|\} \leq \sqrt{n}$ and $max\{|k_{21}|, |k_{22}|\} \leq \sqrt{n}$. Thus, the ISD scalar multiplication kP formula can be expressed as follows:

$$kP = k_{11}P + k_{12}\psi_1(P) + k_{21}P + k_{22}\psi_2(P).$$

The values of sub-scalars k_{11}, k_{12} and k_{21}, k_{22} are computed by solving the shortest vector problem (SVP) in a sub-lattice L_s, that is, a kernel $kerT$ of a homomorphism T of the two dimensional lattice $\mathbb{Z} \times \mathbb{Z}$. The upper bound of the kernel vectors of the ISD reduction map has been found using the characteristic polynomial $p_j(X)$ of

endomorphisms ψ_j for $j = 1,2$ with degree 1 or 2. Based on the distribution of the ISD scalars k in the interval $[1, n-1]$, an increase in the percentage of successful computation of kP of the ISD method compared with the GLV method has been achieved. In this study, the ISD algorithm through the simultaneous computations of the generalization of w_jNAF for $j = 1,2,3,4$ and the extended interleaving algorithms using two models has been implemented. Based on the implementation of the ISD algorithm, ISD computational complexity is determined based on the cost of the elliptic curve and finite field operations through one cycle operation compared with the GLV method.

Most importantly, this work is based on a concrete and strong mathematical foundations that are developed in relation to the proposed idea of the ISD method. Newly developed definitions, theorems, lemmas and corollaries are shown, discussed and proved in this research work. A new modified GLV-ISD method, which combines the GLV and ISD methods, is also proposed to compute the scalar multiplication kP. Using this combined method, most of the percentages of the successful computations of kP have been improved in comparison with GLV or ISD method alone. All algorithms in ISD and hybrid GLV-ISD methods are implemented using Sage software.

CHAPTER 1

INTRODUCTION

1.1 Background

Scalar multiplication techniques on elliptic curves are mostly employed in the area of Cryptography. Cryptography is the science that depends on hard mathematical problems to encrypt and decrypt data. Cryptography protects, stores, and transmits sensitive information across insecure networks so that only specific individuals can decode such information. Cryptography is utilized by spies and has applications in communications (e.g., phone, fax, and e-mail), bank transactions, bank security, passwords, and online credit card transactions.(Hankerson et al., 2004; Cohen et al., 2010; Menezes et al., 2010).

Public key cryptography is a major breakthrough in cryptography. The fundamental feature of the approach is that it does not depend on the same key for encryption and decryption. Public key cryptography has two modes: public and secret (or private) keys. A key is the secret data that is transferred over the network. Public key cryptography, which was introduced by Whitfield Diffie and Martin Hellman in 1976 (Diffie and Hellman, 1976), can solve key distribution problems. Individuals use the public key to convert the data into encrypted form, and only the secret key of the intended user can decrypt such data. This mechanism is also called asymmetric cryptography because of the use of the two keys. Public keys are published

openly, while private keys remain hidden. This technique prevents the leakage of sensitive data from the network. Deducing the private key from the public key is computationally infeasible; only the person with the corresponding private key can decrypt the data. Public key cryptography enables individuals with no pre-existing security arrangements to exchange messages securely.

Elliptic curve cryptography (ECC) was introduced by Victor Miller and Neal Koblitz in 1985 (Miller, 1986; Koblitz, 1987). ECC has attracted researchers, because it has no sub-exponential algorithm, which solves the elliptic curve discrete logarithm problem (ECDLP) on properly chosen elliptic curve (Hao et al., 2008). ECC is currently used as an alternative to Rivest, Shamir and Adleman (RSA) because these methods possess comparable security levels. Several standards organizations also acknowledged ECC as a main public key cryptosystem. Consequently, ECC is ideal for constrained environments such as pagers, personal digital assistants, cellular phones, smart cards and high- bandwidth digital content protection.

In ECC, public and private keys have short lengths. ECC keys are shorter than RSA keys, resulting in faster processing times, and lower memory and bandwidth demands. ECC, requires choosing the type of underlying finite fields and algorithms for implementing finite field arithmetic. The fundamental operations in ECC are point or scalar multiplication kP and multiple point multiplication $lP + mQ$, where k, l and $m \in \mathbb{Z}$. Efficient methods exist for computing kP and $lP + mQ$. The GLV method (Gallant et al., 2001) accelerates scalar multiplication by decomposing a scalar k and using an efficiently computable endomorphism ψ of the elliptic curve E over a prime field F_p. In some cases, the GLV method enables high-degree decompositions in the m-dimensional GLV method (that is, $k_0 + k_1\psi(P) + ... + k_{m-1}\psi^{m-1}(P)$ where

$|k_i| \approx r^{1/m}$) which further accelerates the process.

Several studies have applied the GLV method. However, the main limitation of the method is that it works only for those decomposition values that lie within the range of $\pm\sqrt{n}$. GLV method does not work when the decomposition of a scalar k lies outside the range of $\pm\sqrt{n}$. Therefore, this study proposes a new method called ISD method to solve this problem and to complement the GLV method. The ISD proposes to sub-decompose scalars k_1 and k_2, which form a scalar k, and increase the percentage of successful computations of kP. Consequently, a new and improved version of scalar multiplication on elliptic curves is developed. This newly developed method is called hybrid GLV-ISD scalar multiplication. The GLV-ISD is a combination of the GLV method and the proposed ISD method to compute any multiple kP of point P of order n lying on elliptic curve E over prime field F_p. This new version enhances the existing GLV method by improving the quality of scalar multiplication operations on an elliptic curve. The GLV-ISD method achieves superior increase percentage of the successful scalar multiplications kP computations.

1.2 Elliptic Curve Cryptosystems

Elliptic Curve Cryptosystems based its hardness on the discrete logarithm problem discussed in Hankerson et al. (2004) and are applicable to abstract concepts of finite cyclic groups. The hardness in solving the discrete logarithm problem is for the intractability of the encryption process. The whole computation process involve a mass computation of point multiplications on elliptic curves.

1.2.1 Elliptic Curve Key Generation

Suppose that E is an elliptic curve defined over a finite field F_p and P is a point that lies on E and has prime order n. Point P generates a cyclic subgroup of $E(F_p)$ as follows

$$\langle P\rangle = \{0P,\ 1P,\ 2P,\ 3P, ...,\ (n-1)P\}. \tag{1.1}$$

Public domain parameters consist of $(p,\ E,\ P,\ n)$. Integer d, which is selected uniformly and randomly from interval $[1, n-1]$ is the private key that corresponds to the public key $Q = dP$. For a given domain parameters $(p,\ E,\ P,\ n)$ and Q, the problem of locating d is an elliptic curve discrete logarithm problem (ECDLP). Algorithm (1.12) which is provided in Hankerson et al. (2004) explains how to locate public and private keys in elliptic curve cryptosystems.

1.2.2 Elliptic Curve Encryption and Decryption Schemes

Elliptic curve encryption and decryption are conducted as follows: suppose E is an elliptic curve over F_p and m is a plaintext. First, m should be represented as a point M on elliptic curve E. By randomly choosing integer k, encryption is performed through computations of ciphertext $C_1 = kP$ and $C_2 = M + kQ$. The ciphertext (C_1, C_2) transmits to the recipient via the sender. The recipient uses private key d to compute

$$dC_1 = d(kP) = k(dP) = kQ$$

and then recover $M = C_2 - kQ$. If the eavesdropper wishes to recover M, then the eavesdropper should compute kQ. Computing kQ from Q and $C_1 = kP$ is an

elliptic curve Diffie-Hellman problem. Elliptic curve encryption and decryption are implemented using algorithms (1.13) and (1.14) in Hankerson et al. (2004).

Several criteria motivate the use of elliptic curve families for various applications, one of which is functionality (desired capabilities). All elliptic curve families satisfy desired capabilities in public key cryptography-encryption, signatures, and key agreement. Elliptic curve cryptosystems depend on the hardness of the mathematical problem represented by ECDLP, which is considered the fundamental point for security. Achieving functionality and security affects the performance level of ECC cryptosystems.

ECC has recently attracted researchers because of its short key length requirement. Moreover, ECC boasts high speed and low power consumption (Hankerson et al., 2004). These advantages are useful for some devices like mobile, smartcards, and wireless which, typically, have limited computational resources and bandwidth (Hitchcock and Montague, 2002; Hao et al., 2008; Longa and Gebotys, 2010; Farashahi et al., 2013).

1.3 Why Elliptic Curve Scalar Multiplication?

Elliptic curve arithmetic is an interesting topic for cryptographers, particularly in computing scalar multiplication, which is a core operation in ECC. Scalar multiplication represented by kP for a scalar k is not only the main computational operation in ECC, but also forms a central time-consuming process. Iterative elliptic curve addition (ECADD) and elliptic curve doubling (ECDBL) of points, which are ECC point operations, should be performed to compute scalar multiplication kP. The

efficient performances of these point operations are essential to speeding up scalar multiplication. Therefore, the operational efficiency of scalar multiplication directly determines ECC performance (Rivain, 2011).

1.4 Literature Survey

Several mathematicians have studied the attractive features of elliptic curves for over a hundred years to solve various problems. Elliptic curves were introduced into cryptography by Miller (1986) and Koblitz (1987), who suggested elliptic curve public key cryptosystems. ECC fundamentally computes elliptic curve scalar multiplication kP for a point P, which has a large prime order n. Elliptic scalar multiplication is not only the main computation operation, but also a time-consuming process. Therefore, the operational efficiency of scalar multiplication directly determines ECC performance.

Various methods have been innovated to perform these computations and speed up elliptic curve scalar multiplication. These methods adopted different selections of elliptic curve equations E over various choices of finite fields together with some mathematical conceptions. Some of these methods have determined the work over finite fields with characteristic 2. For example, the study in Koblitz (1992) introduces elliptic curves with complex multiplication. These curves are non-supersingular, which indicates that the reduction of elliptic curve discrete logarithms into finite fields by Menezes-Okamoto-Vanstone is impossible. The groups formed on these curves are ordered and could be factored with large prime numbers. Thus, the Pollard rho method cannot compute a discrete logarithm. Moreover, doubling points can be performed efficiently on these curves. Finally, these curves are easy to locate.

On anomalous curve E, which is defined over binary fields F_2 and binary extension fields F_{2^m} with $m > 1$ by Koblitz (1992), Meier and Staffelbach (1993) proposed a new algorithm to compute multiple k of any arbitrary point on E. The proposed algorithm does not depend on pre-computation values or additional memory and is easy to run. In computing scalar multiplication kP, the proposed algorithm has three times faster executing time than the previous algorithms.

Solinas (2000) improved the algorithm of elliptic scalar multiplication introduced by Meier and Staffelbach (1993) which is a modified version of the Koblitz study. In Solinas (2000), the representation of scalar k in scalar multiplication kP is analogous to binary expansions, which executes the algorithm 50% faster than the previous algorithms. The speed is due to the use of pre-computation values and storage of these values.

A recent new direction has sped up scalar multiplication performance by employing efficiently computable endomorphism of elliptic curve E over prime finite field F_p (Gallant et al., 2001). This method, which is called the GLV method, decomposes multiplier k into a sum of the form $k = k_1 + k_2\lambda \ (mod\ n)$ with $-\sqrt{n} < k_1, k_2 < \sqrt{n}$. The bits of new scalars k_1 and k_2 are half the original bits of k. The simultaneous computation of these new scalar multiplications exhibits a two-fold performance on speed. The decomposition of $k = k_1 + k_2\lambda \ (mod\ n)$ is performed using two linearly independent short vectors in two dimensions, v_1 and v_2 that lie in the kernel of the GLV reduction map $T : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/n$ which is defined by $T(i, j) = i + j\lambda \ (mod\ n)$. This vector set $\{v_1, v_2\}$ forms the GLV generator. The computational efficiency depends on decomposing k into k_1 and k_2 both of which lying within the range of $\sqrt{n}$. The two-dimensional GLV method speeds up the computation by 50%. However, the GLV

generator is claimed experimentally without any proof in the original GLV method (Gallant et al., 2001). Thus, the proof of a necessary condition to fill the gaps on GLV generators in Gallant et al. (2001) was presented in Kim and Lim (2003). The determination of vectors v_1 and v_2 did not guarantee the existence of GLV generators or locating these generators if they do exist. According to the necessary condition of Kim and Lim (2003), the relationship between the components of each vector that form a GLV generator which should be relatively prime has been proven.

The procedure in the GLV method presents a new algorithm based on decomposing multiplier k into the required formula. The extended Euclidean algorithm is used to create a GLV generator. However, the method did not draw explicit bounds of the components in the decomposition, only the estimation to these bounds by $\sqrt{n}$ on several basic implementations. Consequently, an alternative algorithm in Park et al. (2002) is employed to decompose integer k using the theory of μ-Euclidean algorithm. The algorithm decomposes multiplier k according to algebraic number theory and determines the explicit bounds for the components by computing norms in complex quadratic orders. Park et al. (2002) viewed scalar k as an element in $Z[\psi]$, where $Z[\psi]$ is the μ-Euclidean ring and written as $k = \beta\alpha + \rho$, where α, β and ρ in $Z[\psi]$. The computation for elliptic curve scalar multiplication kP is given as $kP = (\beta\alpha + \rho)(P) = \beta(\alpha(P)) + \rho(P) = \rho(P)$. The representation of $\rho = k_1 + k_2\psi$, leads to $kP = \rho P = k_1 P + k_2\psi(P)$. Thus, the alternative algorithm differs from the GLV algorithm through decomposition. Comparing between different decompositions of the same integer k presents no big difference.

Sica et al. (2003) studied the setting of upper bounds for GLV in decomposing scalars k_1 and k_2, which filled the gap in the GLV algorithm. The study presented a

sketched idea of the constant upper bound of the kernel vectors of the GLV reduction map $T(i,j) \rightarrow i + j\lambda \pmod{n}$ through $kP = k_1P + k_2\lambda(P)$ with $max\{|k_1|,|k_2|\} \leq \sqrt{1+|r|+s}\,\sqrt{n}$. The bound in this work is more powerful than the bound in Park et al. (2002).

In Ciet, Lange, Sica and Quisquater (2003), an extended idea of τ-adic expansion on Koblitz curves into a larger class of elliptic curve defined over a prime field which have an efficiently computable endomorphism ϕ is investigated. This extension aims to conduct an efficient scalar multiplication. This study also proposes a combined ϕ-Joint Sparse Form approach, which benefits from the speeding up of the ϕ-expansion and additional speed of Joint Sparse Form (JSF). The algorithm for implementing ϕ-JSF efficiently is employed to compute $a_0P + a_1Q$. The computations are performed by replacing the doubling of endomorphism, which results in one application of ϕ-endomorphism and $l/2$ addition, with l is a bit length of the string that represents a_i for $i = 1,2$.

On the efficient use of computable endomorphisms, Park et al. (2004) expansion method that employs the same kind of endomorphism used by Ciet, Lange, Sica and Quisquater (2003). They presented, on a special type of non-supersingular elliptic curve, the set of all endomorphisms of E, $End(E)$, and the set $\mathbb{Z}[\phi] = \{a + b\phi : a,b \in \mathbb{Z}\}$. ϕ (an endomorphism of E) is an algebraic integer that has the smallest norm in an imaginary quadratic field and is isomorphic. Their study on $\mathbb{Z}[\phi]$ proposed a new division algorithm of scalar k in the scalar multiplication kP through Frobenious endomorphism. They employed ϕ maps instead of point doublings to improve scalar multiplication.

Using an efficiently computable endomorphism defined on a group of elliptic

curve, researchers discovered that some studies derived an efficiently computable homomorphism represented by Frobenious map on a twist of elliptic curves over extension fields F_{p^2} with $j(E) \in F_p$ where $j(E)$ is j-invariant of elliptic curve E. The method presented by Iijima et al. (2002), Iijima, Matsuo, Chao and Tsujii (IMCT), did not apply the GLV method.

The extension of the work in Iijima et al. (2002) is presented by Galbraith et al. (2011). They showed that applying IMCT leads to the GLV method. The Galbraith, Lin and Scott (GLS) approach works only on curves defined on F_{p^m}, where $m > 1$. Their idea was mainly applied on a quadratic twist curve over F_{p^2} of E over F_p. The existence of endomorphism $\psi^2 + r\psi + s = 0$ in the endomorphism ring $End(E)$ is unnecessary, whereas endomorphism in the subgroup $E(F_{p^2})$ is necessary. They identified $\Psi = Frob_p = (x^p, y^p)$ as a Frobenious endomorphism of E over F_p such that $\Psi^m(P) = P$ for all $P \in E(F_{p^m})$. If $P \in E(F_{p^4}) \backslash E(F_{p^2})$ then $\Psi^2(P) = -P$. The subgroup formed by P and Ψ satisfies equation $X^2 + 1 = 0$. The original GLV method is then applied to obtain new scalar multiplication $kP = k_1P + k_2\Psi(P)$, where $max(|k_1|, |k_2|) = O(\sqrt{n})$, if $\Psi(P)$ has a large order n. The work did not focus directly on E/F_{p^4} but on $E^{'}/F_{p^4}$ which is isomorphic to E over F_{p^4} and not over F_{p^2}, and thus, on the a quadratic twist curve over F_{p^2}. The order of points $\#E^{'}(F_{p^2}) = n \geq (p-1)^2$ is prime. If $\psi : E^{'} \rightarrow E$ is an isomorphism defined over F_{p^4}, then the endomorphism $\Psi = \psi Frob_p \psi^{-1} \in End(E^{'})$ satisfies equation $X^2 + 1 = 0$. ψ can be defined on F_p if $p \equiv 5 \ (mod \ 8)$. The four dimensional of GLV method (4-GLV) on curves with nontrivial automorphism of one degree is presented also in this study.

The 4-GLV, presented by Longa and Sica (2012). The new approach is a combination between the two approaches; (1) the original GLV over F_p, which is

defined by this formula

$$kP = k_1P + k_2\Phi(P) \text{ with } max(|k_1|,|k_2|) < C_1\sqrt{n},$$

for some constant $C_1 > 0$ and (2) the GLS approach, presented by Galbraith et al., which works with twists curves over F_{p^2} of curves defined over Fp. The new hybrid approach utilizes two fast endomorphisms Φ and Ψ over F_{p^2}, which are applied on the group generated by elliptic curve point P which has a prime order n. This procedure forms a four dimensional decomposition, which takes this expression

$$kP = k_1P + k_2\Phi(P) + k_3\Psi(P) + k_4\Psi\Phi(P) \text{ with } max(|k_i|) < C_2n^{1/4}, i = 1,2,3,4,$$

for any scalar $k \in [1, n-1]$ and a constant $C_2 > 0$. The study determines the choice of the best constants, C_1 and C_2 through this relationship $C_2/C_1 < 408$. Choosing constants is independent of choice curve, which are guaranteed to constantly speed up. Another type of endomorphism with degree 3 is employed to derive new families of the GLV curves.

The study of Galbraith et al. (2011) left some open problems, one of which is the study of the GLV method in 4-dimensions on special curves with $j(E) = 0$ over F_{p^2} where $j(E)$ is j-invariant of elliptic curve E. In Hu et al. (2012), the curves showed a reduction of the number of doublings for point multiplication up to a quarter through the application of the 4-dimension of GLV with suitable decomposed coefficients. This implementation reduced 27% of the time used to implement other fast algorithms of point multiplication presented by Longa and Gebotys (2010).

The protection of elliptic scalar multiplication against differential power attack

(DPA) is proposed, employing a new method by Ciet, Quisquater and Sica (2003). This protection benefits from the speed of the GLV method in two dimensions to randomize scalar k of scalar multiplication kP. Two variants are proposed from applying this new protection method: linear and affine. The affine method is more effective than the linear method. Protecting computations of elliptic curves by improving the performance of side channels is presented in (Faz-Hernández et al., 2014).

New efficient algorithms used the GLV scalar multiplication proposed in (CRYPTO 2001) and Galbraith-Lin-Scott in (EUROCRYPT 2009) are discussed. A new signed representation on the GLV setting is employed to produce a new method for computing scalar multiplication, which employs the GLV idea. This method is called the GLV-based sign-aligned column (GLV-SAC). A sign representation in the GLV-SAC method takes a different form compared to traditional sign representations (e.g., interleaving or joint sparse form). GLV-SAC employs the recoding that proposed in Feng et al. (2005), for computing the GLV scalar multiplication through a variable-base. GLV-SAC can resist attacks including the simple power attack.

Wang et al. (2012) presented the study for forming a reduced lattice basis. On sub-lattice L_s of lattice L, a reduced lattice basis can be constructed using two polynomials that form a Sylvester matrix. The reduced lattice, with some special properties, can be applied on the n-GLV method to compute scalar multiplication on GLS curves.

Smith (2013) proposed a new study to implement GLV, GLS, GLV+GLS, and the constructions of the $\mathbb{Q}$-curve on elliptic curves and the constructions of genus 2 real multiplication. The quadratic rings form a short basis of the lattice. The proposed method constructs superior scalar decompositions.

On the three dimensional (3-GLV) method, Zhou et al. (2010) presented a new study that employed two distinct endomorphisms of Galbraith-Lin-Scott (GLS) that defined in Galbraith et al. (2011). These endomorphisms generalized the 2-GLV method introduced in Gallant et al. (2001), and the results ensure that the 3-GLV method executes with 0.897 the time to implement the 2-GLV method according to Galbraith et al. (2011) for computing scalar multiplication kP on GLS curves.

The study used the curves introduced by Bos et al. (2013) have genus 2 over quadratic extension fields to benefit from these curves and obtain 8-dimensional GLV method through the combined GLV-GLS algorithm. The algorithm can perform computations in a 64-bit characteristic field, which is attractive for embedded devices.

In Longa and Sica (2014), the combination of the GLV method by Gallant et al. (2001) applied on elliptic curve E over a prime field F_p

$$kP = k_1P + k_2\psi(P), \text{ with } max\{|k_1|,|k_2|\} \leq C_1\sqrt{n},$$

and the study in Galbraith et al. (2011) is applied on the twists of elliptic curve E over extension prime field F_{p^2} to decompose scalar k in four dimensions by using efficiently computable endomorphisms ϕ and Φ over F_{p^2}. These endomorphisms are acted on the subgroup generated by generator point P on E, which has prime order n. The formula of 4-GLV scalar multiplication is provided by

$$kP = k_1P + k_2\Phi(P) + k_3\Psi(P) + k_4\Psi\Phi(P) \text{ with } max(|k_i|) < C_2n^{1/4}, i = 1,2,3,4,$$

for some $k \in [1, n-1]$ and for some constant $C_2 > 0$. The best constants are chosen to produce $C_2/C_1 < 412$ regardless of the curve. Choosing these constants is

important because it affects the speed of the computations. The merged GLV-GLS method shows a faster running time of up to 50% than the original GLV method. Exploiting the twisted Edwards curves on the GLV-GLS method further improved the performance. The performance of the GLV-GLS method is assessed to protect the GLV scalar multiplication efficiently against several side channel attacks through several measurements.

1.5 Problem Statement

Recent studies for computing scalar multiplication kP depend on the decomposition of scalar k using efficiently computable endomorphisms ψ of elliptic curve E over prime finite field F_p. The decomposition of scalar k, where k is a positive integer that lies in the interval $[1, n-1]$, produces new scalars k_1 and k_2 with $|k_1|, |k_2| < \sqrt{n}$. Scalar k is written by the formula $k \equiv k_1 + k_2\lambda \ (mod\ n)$, with $|k_1|$ and $|k_2|$ lying within the range $\sqrt{n}$ on the interval $[1, n-1]$ and $\lambda \in [1, n-1]$, which was proposed by Gallant et al. (2001). However, looking closely on the same interval $[1, n-1]$ that contains scalars k the existing decomposition method did not consider those k for which it decomposes into new scalars $|k_1|$ and $|k_2|$ with one or both new scalars lie outside the range of $\sqrt{n}$ on the interval $[1, n-1]$. This point is a major gap in Gallant et al. (2001) because any decomposition produces new scalars $|k_1|$ and $|k_2|$ outside the range of $\sqrt{n}$ such that $max\{|k_1|, |k_2|\} > \sqrt{n}$, indicates that the GLV method cannot be applied.

Several researchers have conducted improvements on computing scalar multiplication on the basis of the GLV method starting in the year 2001. The GLV decomposition of scalar k is presented in various dimensions: two, three, four, eight and n- dimensional GLV methods (2-GLV,3-GLV, 4-GLV,8-GLV and n-GLV). The

decomposition speeds up the computation of scalar multiplication kP. All previous studies have gaps in the decomposed scalars $|k_1|$ and $|k_2|$ which lie outside the range of $\sqrt{n}$ that satisfies $max\{|k_1|,|k_2|\} > \sqrt{n}$. Another aspect that was not considered in the previous decomposition methods is the limited number of k in the interval $[1,n-1]$ for which the decomposition values lie within the given range. This resulted in a low percentage of successful computation of kP, for k in the interval $[1,n-1]$. These two main problems determine the objectives of this research work.

1.6 Research Objectives

The objectives of this study are:

i. To propose a new method, namely the integer sub-decomposition (ISD) method, which complements the GLV method in computing elliptic curve scalar multiplication kP; the decomposition of scalar k provides a maximum value of integers $|k_1|$ and $|k_2|$, which lie outside the range $\sqrt{n}$ on interval $[1,n-1]$ and increases the percentage of successful computation kP on interval $[1,n-1]$.

ii. To generalize, to extend and to generate important properties related to the new proposed ISD method.

iii. To establish the upper bound of the ISD elliptic curve scalar decomposition values.

iv. To study the distribution of scalar k for the ISD method in the interval $[1,n-1]$ for various values of n.

v. To compute the computational complexity of the ISD method and compare the computational complexity of the GLV and ISD elliptic curve scalar

multiplication methods in one cyclic operation.

vi. To implement the ISD algorithm through simultaneous computing the generalization of w_j-NAF, with $j = 1,2,3,4$, where w_j-NAF are window non adjacent forms to represent sub-scalars of ISD method, namely k_{11}, k_{12}, k_{21} and k_{22} and the extended interleaving algorithms.

vii. To develop a new approach called, the GLV-ISD method, which combines the GLV method and the proposed ISD method.

1.7 Methodology

To be able to achieve the objectives of this work, several important steps and methodology has to be determined here. The following shows the step by step method in order to achieve each objective.

Generalization, extension and generation of several important properties related to ISD method

Step 1 Let n and λ_j for $j = 1,2,...,m$ be two positive integers not both zero, namely $n \neq 0$ or $\lambda_j \neq 0$ and $n \geq \lambda_j$. Generalize the extended Euclidean algorithm to locate m-tuples of variables r_j, t_j and s_j on the basis of the generalization of the division algorithm, Euclidean algorithm, and some other definitions.

Step 2 Let E be an ordinary elliptic curve over F_p and $P \in E(F_p)$ be a point that has a large prime order n and assume that λ_1 and $\lambda_2 \in [1, n-1]$, where $\lambda_1 \neq \pm\lambda_2$. Locate the linearly independent integer vectors v_3, v_4 and v_5, v_6 in the kernel T

by generalizing the extended Euclidean algorithm.

Step 3 Let E be an ordinary elliptic curve over F_p and $P \in E(F_p)$ be a point that has a large prime order n, λ_1 and $\lambda_2 \in [1, n-1]$, where $\lambda_1 \neq \pm\lambda_2$ and the linearly independent integer vectors v_3, v_4 and v_5, v_6 are in the kernel of T. Locate two ISD generators $\{v_3, v_4\}$ and $\{v_5, v_6\}$ which satisfy the necessary conditions that the relationship between components for each vector v_i, for $i = 1, 2, 3, 4$ are relatively prime and on each vector, the components are less than $\sqrt{n}$.

Generating the ISD decomposition values

Step 1 Let E be an ordinary elliptic curve over F_p, such that $\#E(F_p) = p + 1 - t$ with $|t| \leq 2\sqrt{p}$ and P is a point lying on E has a large prime order n and $k \in [1, n-1]$. Assume that $\{v_3, v_4\}$ and $\{v_5, v_6\}$ are ISD generators and the decomposition of scalar k produces the maximum value of integers k_1 and k_2 that lie outside the range of $\sqrt{n}$. Sub-decompose k_1 and k_2 into k_{11}, k_{12}, k_{21} and k_{22} with $max\{|k_{11}|, |k_{12}|\} \leq \sqrt{n}$ and $max\{|k_{21}|, |k_{22}|\} \leq \sqrt{n}$.

Step 2 Let E be an ordinary elliptic curve over F_p, such that $\#E(F_p) = p + 1 - t$ with $|t| \leq 2\sqrt{p}$ and P be a point lying on E that has a large prime order n and $k \in [1, n-1]$. Assume that $\{v_3, v_4\}$ and $\{v_5, v_6\}$ are ISD generators and the decomposition of a scalar k produces the maximum value of integers $|k_1|$ and $|k_2|$ that lie outside the range of $\sqrt{n}$ on the interval $[1, n-1]$. The ISD sub-decomposition of k_1 and k_2 is k_{11}, k_{12}, k_{21} and k_{22} with $max\{|k_{11}|, |k_{12}|\}$ and $max\{|k_{21}|, |k_{22}|\} < \sqrt{n}$. Compute a scalar multiplication

elliptic curve $kP = k_{11}P + k_{12}\psi_1(P) + k_{21}P + k_{22}\psi_2(P)$, with $max\{|k_{11}|, |k_{12}|\} \leq \sqrt{n}$ and $max\{|k_{21}|, |k_{22}|\} \leq \sqrt{n}$.

Establishing upper bounds for the ISD pairs, $\{k_{11}, k_{12}\}$ ***and*** $\{k_{21}, k_{22}\}$

Let E be an ordinary elliptic curve defined over F_p and P be a point lying on E that has a large prime order n and $k \in [1, n-1]$. Assume that the ISD scalar multiplication is defined to compute kP. Fill the gap with the proof of the upper bound of kernel vectors of the ISD reduction maps $T : (a,b) \rightarrow a + \lambda_j b (mod\ n)$ with $j = 1, 2$, through the determination of explicit constants in this bound to become ISD scalar multiplication as $kP = k_{11}P + k_{12}\psi_1(P) + k_{21}P + k_{22}\psi_2(P)$, with $max\{|k_{11}|, |k_{12}|\} < \sqrt{1 + |\lambda_j|}\ \sqrt{n}$ and $max\{|k_{21}|, |k_{22}|\} < \sqrt{1 + |\lambda_j|}\ \sqrt{n}$, for $j = 1, 2$.

Distribution of the scalar k ***for the ISD method***

Let E be an ordinary elliptic curve over F_p, such that $\#E(F_p) = p + 1 - t$ with $|t| \leq 2\sqrt{p}$ and P be a point lying on E that has a large prime order n and $k \in [1, n-1]$. Assume that ISD elliptic scalar multiplication is defined. Investigate the distribution of scalar k in the ISD computation in the interval $[1, n-1]$ for various values of n. From the distribution of k, successful percentage of computation of kP can be obtained and comparison are made between the ISD and the GLV methods.

Simultaneous computation using models based on interleaving method

Let E be an ordinary elliptic curve over F_p, such that $\#E(F_p) = p + 1 - t$ with $|t| \leq 2\sqrt{p}$ and P be a point lying on E that has a large prime order n and $k \in [1, n-1]$. Assume that ISD elliptic scalar multiplication is defined. Execute the performance of the ISD method through simultaneous computations using two new models based

on the interleaving methods, which employ the generalization of width w-NAF expansions.

Complexity computation of the ISD method

Step 1 Let E be an ordinary elliptic curve over F_p, such that $\#E(F_p) = p+1-t$ and P be a point lying on E that has a large prime order n and $k \in [1, n-1]$. Assume that ISD elliptic scalar multiplication is defined. Compute the computational complexity of the ISD algorithm.

Step 2 Let E be an ordinary elliptic curve defined over F_p and P be a point lying on E that has a large prime order n and $k \in [1, n-1]$. Assume that the GLV and ISD scalar multiplication are defined to compute kP and determine the computational costs of these methods. Compare these methods in terms of the computational complexity of each technique in one cycle operation.

Implementation of GLV-ISD method

Let E be an ordinary elliptic curve defined over F_p and P be a point lying on E that has a large prime order n and $k \in [1, n-1]$. Assume that the GLV and ISD scalar multiplication are defined to compute kP. Incorporate the GLV and ISD methods to create a new approach, the GLV-ISD method, which increases the percentage of successful computation of scalar multiplication kP.

1.8 Thesis Contribution

The results are mostly included in Chapters 3, 4, 5, 6, and 7. The most important contributions are as follows:

i. a new method called integer sub-decomposition (ISD), to compute scalar multiplication on elliptic curve E over prime field F_p through theoretical proofs, new algorithms, and practical implementation results.

ii. the theoretical proof and practical implementation of the upper bound to the kernel vectors of the ISD reduction map determine the upper bound of the ISD sub-scalars, which form the original scalar k of scalar multiplication kP on elliptic curve E over prime F_p.

iii. the probability distribution of the GLV and ISD scalars k in various interval $[1, n-1]$ with n as the prime number is determined, which assists in computing the rates and percentages of these methods.

iv. the ISD algorithm is applied. Two models are employed for the computation of scalar multiplication kP through the interleaving method, which is based on wNAF expansions in parallel computation.

v. the computational complexity of the ISD computation method is determined, which depends on elliptic curve operations and finite field operations that design the computation of the running time of scalar multiplication

vi. a new modified method is proposed for scalar multiplication on an elliptic curve, which is called GLV-ISD scalar multiplication. The GLV-ISD method is a

combination of the GLV and ISD methods for computing any multiple kP of point P of order n, which lies on an elliptic curve E over prime field F_p.

Figure (1.1) shows the important contributions of this work.

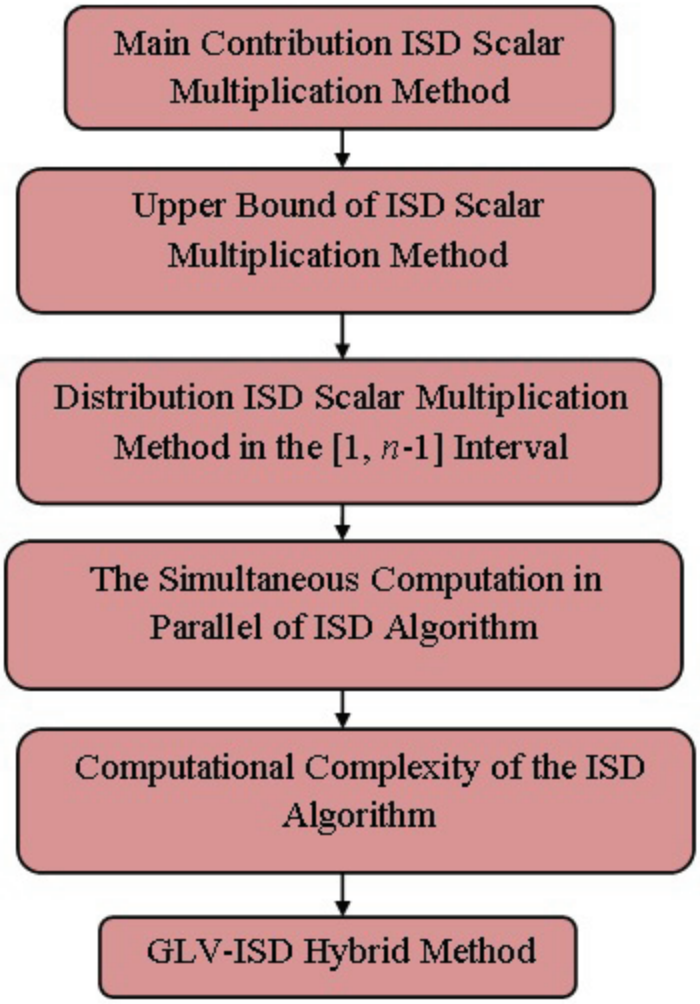

Figure 1.1: The contributions of the thesis.

1.9 Thesis Organization

The thesis outline is as follows:

- **Chapter 1:** includes a basic introduction to cryptography, presenting discrete logarithm and elliptic curve systems. The chapter presents a literature survey of previous studies on elliptic curve scalar multiplication over finite fields. The chapter presents the problem statements, objectives methodology, contribution, and organization of the thesis.

- **Chapter 2:** presents mathematical foundations in algebra and number theories, including Euclidean and extended Euclidean algorithms, and finite fields (e.g., prime fields). The chapter introduces lattices in two dimensions. The chapter presents the study of elliptic curves over prime fields. Endomorphisms and Frobenius endomorphism are discussed. The chapter discusses important scalar multiplication methods, particularly the Gallant, Lambert and Vanstone (GLV) method, which utilizes efficient computable endomorphism of elliptic curve E. The chapter also presents significant methods in computing multiple scalar multiplication (e.g., SMSM and interleaving method).

- **Chapter 3:** discusses the proposed integer sub-decomposition (ISD) method for computing scalar multiplication kP on elliptic curves E, which employs efficiently computable endomorphisms over prime field F_p to complement the GLV method and increase the percentage of successful computation scalar multiplication kP. The chapter also generalizes definitions, theorems, and algorithms (e.g., division algorithm, Euclidean algorithm, extended Euclidean

algorithm, and width-w NAF algorithm) which provides the theoretical proof of the ISD method.

- **Chapter 4:** discusses and proves the value C in the upper bound of the GLV method. The procedure in finding C in the upper bound of the ISD method is also discussed and proved to determine the upper bound of the ISD method. The distribution of the scalar in the original 2-GLV and 2-ISD computation methods is presented. The comparison of the percentages of successful computations of kP on ISD and GLV methods is introduced.

- **Chapter 5:** presents the application of two new models for improving the performance of the ISD scalar multiplication method through simultaneous computation. The chapter introduces two simultaneous ways for computing the width-wNAF algorithm in representing positive integers. The chapter discusses two new models for computing the interleaving method.

- **Chapter 6:** includes the computational complexity of the 2-ISD method. The computational cost of group law for prime curve is presented in the first part. The computational complexity of the GLV method is presented in the second part. The chapter discusses the computational complexity of the ISD method. The comparison between the GLV and ISD methods in one cycle operation is presented in the last part.

- **Chapter 7:** describes the combined GLV-ISD method, which comprises two main parts: the GLV (introduced in 2001) and ISD (newly developed in this work). The distribution of scalars k in the GLV-ISD computation method on interval $[1, n-1]$ is determined. The computational complexity of the

combined GLV-ISD method is addressed. The comparison of the percentages of successful computations of kP on GLV, ISD and GLV-ISD methods is presented. This chapter displays simultaneous computation of the GLV-ISD method in computing scalar multiplication kP and computational complexity simultaneous computation. The experimental results of the GLV-ISD method are introduced.

- **Chapter 8:** draws the conclusion and discusses possible research trends and future work.